

#5

Docket No.: 62807-040

PATENT

## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Yoko KUMAGAI, et al.

Serial No.: 10/076,624

Group Art Unit: 2131

Filed: February 19, 2002

Examiner:

For: PUBLIC KEY CERTIFICATE GENERATION METHOD, VALIDATION  
METHOD AND APPARATUS THEREOFTRANSMITTAL OF CERTIFIED PRIORITY DOCUMENTHonorable Commissioner for Patents and Trademarks  
Washington, D. C. 20231

Sir:

At the time the above application was filed, priority was claimed based on the following application:

**Japanese Patent Application Number 2001-356851, Filed November 22, 2001**

A copy of each priority application listed above is enclosed.

Respectfully submitted,

MCDERMOTT, WILL &amp; EMERY

A handwritten signature in black ink, appearing to read "KEITH E. GEORGE".

Keith E. George  
Registration No. 34,111

600 13<sup>th</sup> Street, N.W.  
Washington, DC 20005-3096  
(202)756-8000 KEG:kjw  
Facsimile: (202)756-8087  
**Date: June 28, 2002**

Docket No.: 62807-040

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Yoko KUMAGAI, et al.

Serial No.:

Filed: February 19, 2002

Group Art Unit:

Examiner:

For: PUBLIC KEY CERTIFICATE GENERATION METHOD, VALIDATION METHOD  
AND APPARATUS THEREOF

JC979 U.S. PRO  
10/076624  
02/19/02



CLAIM OF PRIORITY

Commissioner for Patents  
Washington, DC 20231

Sir:

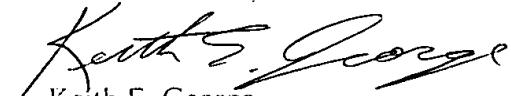
In accordance with the provisions of 35 U.S.C. 119, Applicant hereby claims the priority of:

**Japanese Patent Application Number 2001-356851, File November 22, 2001**

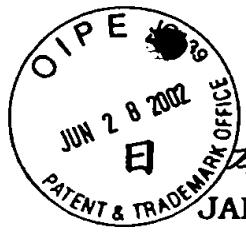
cited in the Declaration of the present application. A Certified copy will be filed in due course.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

  
Keith E. George  
Registration No. 34,111

600 13<sup>th</sup> Street, N.W.  
Washington, DC 20005-3096  
(202) 756-8000 KEG:kjw  
**Date: February 19, 2002**  
Facsimile: (202) 756-8087



日本国特許庁  
JAPAN PATENT OFFICE

62807-040  
YOKO Kumaqai, et al  
February 19, 2002  
10/076,624  
MIE & E

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2001年11月22日

## 出願番号

**Application Number:**

特願2001-356851

[ ST.10/C ]:

1

[ J P 2 0 0 1 - 3 5 6 8 5 1 ]

## 出願人

**Applicant(s):**

株式会社日立製作所

**CERTIFIED COPY OF  
PRIORITY DOCUMENT**

**CERTIFIED COPY OF  
PRIORITY DOCUMENT**

2002年 2月22日

特許庁長官  
Commissioner,  
Japan Patent Office

# 及川耕造

【書類名】 特許願  
【整理番号】 K01011441A  
【あて先】 特許庁長官  
【国際特許分類】 H04L 12/00  
【発明者】  
【住所又は居所】 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所 システム開発研究所内  
【氏名】 熊谷 洋子  
【発明者】  
【住所又は居所】 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所 システム開発研究所内  
【氏名】 藤城 孝宏  
【発明者】  
【住所又は居所】 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所 システム開発研究所内  
【氏名】 手塚 哲  
【発明者】  
【住所又は居所】 東京都江東区新砂一丁目6番27号 株式会社日立製作所 公共システム事業部内  
【氏名】 及川 隆信  
【発明者】  
【住所又は居所】 東京都江東区新砂一丁目6番27号 株式会社日立製作所 公共システム事業部内  
【氏名】 穴山 泉  
【特許出願人】  
【識別番号】 000005108  
【氏名又は名称】 株式会社日立製作所  
【代理人】  
【識別番号】 100075096

【弁理士】

【氏名又は名称】 作田 康夫

【手数料の表示】

【予納台帳番号】 013088

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 公開鍵証明書の生成方法、検証方法、および装置

【特許請求の範囲】

【請求項1】

公開鍵基盤における、登録機関と発行機関による公開鍵証明書の生成方法であって、

前記登録機関において、公開鍵証明書への登録内容と、当該登録内容のうち当該登録機関が保証する情報と、添付した証明書発行依頼を、前記発行機関に送り、

前記発行機関において、前記証明書発行依頼に記載された前記登録内容と、前記登録機関が保証する情報と、当該発行機関での発行内容と、当該発行内容に対する署名とからなる公開鍵証明書を生成することを特徴とする公開鍵証明書の生成方法。

【請求項2】

請求項1記載の公開鍵証明書の生成方法であって、

前記公開鍵証明書に記載される情報を指定する識別子を予め定め、

前記登録機関は、前記登録機関が保証する情報に対する署名と、前記保証する情報を指定する識別子とを、前記登録機関が保証する情報に含めることを特徴とする公開鍵証明書の生成方法。

【請求項3】

請求項1記載の公開鍵証明書の生成方法であって、

前記登録機関は、当該登録機関が保証する情報にハッシュ関数を作用させたハッシュ値を求め、当該ハッシュ値に対する署名を生成し、前記ハッシュ値と前記署名とを、前記登録機関が保証する情報に含めることを特徴とする公開鍵証明書の生成方法。

【請求項4】

請求項1に記載された公開鍵証明書の生成方法に従って生成された公開鍵証明書の検証方法であって、

検証者は、前記公開鍵証明書全体に対して付与された前記発行機関の署名と、

前記登録機関の署名とを検証し、

前記登録機関が署名した登録内容と前記発行機関が署名した発行内容とを確認する

ことを特徴とする公開鍵証明書の検証方法。

【請求項5】

請求項2に記載された公開鍵証明書の生成方法に従って生成された公開鍵証明書の検証方法であって、

前記検証者は、前記識別子に従い、前記登録機関が署名対象とした情報を公開鍵証明書から取得し、

取得した前記情報のハッシュ値を求め、

前記登録機関が保証する情報に含まれる前記登録機関の署名を当該登録機関の公開鍵で復号化し、

前記ハッシュ値と前記復号化した値とが等しいかどうかを調べ、前記登録機関が保証対象とする情報の検証を行う

ことを特徴とする公開鍵証明書の検証方法。

【請求項6】

請求項3に記載された公開鍵証明書の生成方法に従って生成された公開鍵証明書の検証方法であって、

前記公開鍵証明書に記載された情報のハッシュ値を求め、

前記登録機関が保証する情報に含まれるハッシュ値と、前記求めたハッシュ値とを比較し、

前記登録機関が保証対象とする情報の識別と識別した情報の検証とを行うことを特徴とする公開鍵証明書の検証方法。

【請求項7】

請求項4に記載された公開鍵証明書の検証方法であって、

前記検証者が信頼する認証局から、前記公開鍵証明書までのパス構築と当該パスの検証を行い、

前記公開鍵証明書に記載された、前記登録機関の署名を、当該登録機関の公開鍵で検証し、

前記検証者が信頼する前記認証局から前記登録機関の公開鍵証明書までのパス構築と検証を行う

ことを特徴とする公開鍵証明書の検証方法。

【請求項8】

請求項7に記載の公開鍵証明書の検証方法であって、

前記認証局から前記登録機関の公開鍵証明書までのパス構築において、

前記検証者は、検証対象の公開鍵証明書に記載された登録機関名に基づいて、当該発行機関の公開鍵証明書データベースから、前記登録機関の公開鍵証明書を取得する

ことを特徴とする公開鍵証明書の検証方法。

【請求項9】

請求項7に記載の公開鍵証明書の検証方法であって、

前記認証局から前記登録機関の公開鍵証明書までのパス構築において、

前記検証対象の公開鍵証明書の拡張領域に記載された前記登録機関の公開鍵証明書を取得する

ことを特徴とする公開鍵証明書の検証方法。

【請求項10】

請求項1に記載された公開鍵証明書の生成方法に従って生成された公開鍵証明書の失効方法であって、

前記登録機関は自身の公開鍵証明書の発行機関へ証明書失効要求を送付し、

前記発行機関は、前記証明書失効要求を受け取り、前記登録機関の公開鍵証明書を失効させ、

前記登録機関が登録を行った公開鍵証明書を失効させる  
ことを特徴とする公開鍵証明書の失効方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、公開鍵基盤（PKI（Public Key Infrastructure））に於ける、公開鍵証明書を発行する技術と、その公開鍵証明書の有効性を確認する技術とに関する

## 【0002】

## 【従来の技術】

電子文書などディジタルデータを送付する際に、対象となるデータに対して、署名と送信者の公開鍵証明書を添付することが行われる。受信者では、受信データに添付されたディジタル署名（以下署名という）と公開鍵証明書の検証を行い、送付されたデータが改ざんされていないことと、確かに本人から送られた電子データであることを確認する。

## 【0003】

公開鍵証明書の発行と有効性の確認は、公開鍵基盤において行われ、その標準仕様はRFC2459 (Internet X.509 Public Key Infrastructure Certificate and CRL Profile) や、RFC2510 (Internet X.509 Public Key Infrastructure Certificate Management Protocols) 等にて規定されている。

## 【0004】

RFC2459 (3章) や、RFC2510 (1. 3) の構成モデルに示されるように、認証局の業務は主に、登録業務と発行業務から構成される。登録業務とは、利用者の登録ならびにその審査を行う業務であり、登録機関 (Registration Authority、以下RAという) において行われる。

## 【0005】

発行業務とは主に、登録された利用者に対する公開鍵証明書の発行を行う業務であり、発行機関 (Issuing Authority、以下IAという) によって行われる。

## 【0006】

なお、RFC2459およびRFC2510では、発行業務を行う機関を認証局 (Certificate Authority、以下CAという) と定義しているが、本明細書においていは、発行業務を行う機関を発行機関IAと定義し、CAはRAとIAとからなると定義する。

## 【0007】

発行業務は、セキュアな設備や機器を必要とするため、高い維持費用と構築費用を要する。そのため、認証局を構築する組織は、発行業務処理を外部へ委託（

以下、アウトソーシング（outsourcing）というする場合がある。

【0008】

従来、発行業務をアウトソーシングする次の2つの方法がある。

【0009】

方法1では、認証局を構築する組織は、エンドエンティティ（End Entity、以下E Eという。利用者やエンドユーザともいう）の本人確認や審査を、自機関のR Aで行い、IAの業務全般（機器、設備、IAの運用等）を他機関へアウトソーシングする。アウトソーシング先機関は、複数のR Aの公開鍵証明書発行業務を代行する。このとき、アウトソーシング先機関の秘密鍵が公開鍵証明書の発行に用いられ、アウトソーシング先機関名が公開鍵証明書発行者名（Issuer）として記載される。

【0010】

方法2では、認証局を構築する組織は、RAの業務を自機関で行い、IAの機器管理等の業務を他機関へアウトソーシングする。そこでは、認証局を構築する組織毎に専用のIAの機器や秘密鍵が用いられる。例えば、異なるRA毎のIAとIA秘密鍵とが、アウトソーシング先機関へ設けられる。この場合、認証局を構築する組織名（RA運営者名）が公開鍵証明書発行者名（Issuer）として記載される。

【0011】

以上の二つの方法が採用されている例として、日本認証サービス株式会社（J C S I）のS e c u r e S i g nという証明書発行サービスがある。J C S Iの「S e c u r e S i g nパブリックサービス標準規定（V1. 0）」（J C S I, S e c u r e S i g nは、日本認証サービス株式会社の登録商標である）5ページには、以下のことが記述されている。

【0012】

S e c u r e S i g nには、「パブリックサービス」「プライベートサービス」という二種類のサービスがある。プライベートサービスの場合、証明書ポリシーならびにC P Sは顧客により決定され、顧客が必要とするネットワーク上のドメイン内に開示される。一方、パブリックサービスでは、J C S Iがパブリック

サービスの証明書発行者であり、証明書に署名する当事者であるということを意味する。

【0013】

【発明が解決しようとする課題】

発行業務と登録業務とを異なる組織で運営すると、利用者に対するIAとRAの責任範囲が明確にならないという問題点がある。IAとRAの責任範囲は、認証局運用規程 (Certificate Practice Statement、以下CPSという) 等で明確にすることとなっている。しかし発行された公開鍵証明書の内容において生じた問題（例えば、記載事項に間違いがあった場合など）の責任の所在を判断するには、IAやRAの内部データ（ログ等）を調べる必要があり、判断が難しい、時間がかかる、などの問題がある。

【0014】

【課題を解決するための手段】

本発明は、複数の当事者機関が作成に係わる公開鍵証明書について、公開鍵証明書の内容に対する各当事者の責任範囲を明確にする技術を提供する。

【0015】

また、本発明は複数の当事者機関が作成に係わる公開鍵証明書の検証技術を提供する。

【0016】

また、本発明は複数の当事者機関が作成に係わる公開鍵証明書について、その内容を利用者に分かりやすく示す技術を提供する。

【0017】

また、本発明は、上記技術に基づいた、公開鍵証明書の発行、登録、検証に係わる装置、またはそれらの装置を用いたシステム、または、各装置やシステムで用いられる処理方法を提供する。

【0018】

具体的には、本発明では、発行業務全般を他機関へアウトソーシングする場合において、以下のような公開鍵証明書発行の処理および検証処理を行う。

【0019】

本発明における公開鍵証明書の発行処理において、次の処理を行う。

#### 【0020】

RA装置は、RAにおいて行われるEEの本人確認、審査等の後、EEがもつ情報のうち、公開鍵証明書に記載する情報、例えばEE名(subject)、公開鍵(subjectPublicKeyInfo)、に対してその内容を保証するRAの署名を生成する。RAは、生成したRA署名を添付した公開鍵証明書発行要求をIAへ送付する。

#### 【0021】

IAがRAから受け取った公開鍵証明書発行要求に応じて、IA装置は公開鍵証明書を作成する。公開鍵証明書にはRAの名前とRAの署名とその署名対象情報が格納され、公開鍵証明書全体に対するIAの署名が生成され付与される。

#### 【0022】

上記手順で発行されたEEの公開鍵証明書の効力を停止するには、その登録に係わったRAの公開鍵証明書を失効させればよい。具体的には、RA装置は自身の公開鍵証明書の発行機関へ証明書失効要求を送付する。それを受け取ったRAの公開鍵証明書の発行機関は、RAの証明書を失効させる(失効リストに載せる)。この方法は、例えば、RAの運営終了時等に、RAが登録を行った全てのEEの公開鍵証明書を、一括して失効させる場合などに有効である。

#### 【0023】

本発明による公開鍵証明書を、取引の過程などで受け取ったEEは、その公開鍵証明書を検証するために、次の検証処理を行う。

#### 【0024】

まず、EE装置は、検証を行うEEが信頼する認証局の自己署名証明書から、当該公開鍵証明書までのパス構築およびパス検証を行う。次に、公開鍵証明書に記載されたRAの署名を、RAの公開鍵で検証する。そして、検証を行うEEの信頼する認証局の自己署名証明書から、RAの公開鍵証明書までのパス構築および検証を行う。この際、RAの公開鍵証明書が失効していた場合、検証対象の公開鍵証明書は有効でないものとなる。

#### 【0025】

本発明による公開鍵証明書には、RAの名前と、署名と、検証者が署名による保証対象を知ることができる情報とが記載されているので、公開鍵証明書を受け取ったEEは、RAが何を保証しているのかを知ることができる。RAの保証範囲以外の記載事項は、IAが保証していることになり、この結果、IAとRAの責任範囲を明確化することができる。

## 【0026】

## 【発明の実施の形態】

図1は、本発明の実施形態が適用されたPKIシステムの概略構成を示す図である。

## 【0027】

本実施例のPKIシステムは、電子的に手続を行うEE1装置(15)、EE2装置(16)(EE装置と総称する)と、公開鍵証明書発行業務を行うCA1装置(13)、CA2装置(14)(CA装置と総称する)と、それぞれを接続するインターネット等のネットワーク(以下、NETという)17からなる。CA装置1(13)は、登録業務を行うRA装置(11)と、公開鍵証明書の発行業務と管理を行うIA装置(12)とから構成され、それぞれがNET(17)に接続されている。

## 【0028】

NET(17)を介して互いに接続しているIA装置(12)とRA装置(11)は、論理的にはCA1(13)を構築するものであれば、物理的に同じ場所にある必要はない。

## 【0029】

さらに、CA1装置(13)を運営する組織は、IA装置(12)を用いたIA業務を別機関にアウトソーシングしているため、IA装置(12)とRA装置(11)を運営する組織は異なるものとする。

## 【0030】

また、点線で示すように、CA1(13)は、CA2(14)と相互認証し、CA1(13)は、EE1(15)に対してその公開鍵証明書を発行し、CA2(14)は、EE2(16)に対してその公開鍵証明書を発行するものとする。

EE1(15)、EE2(16)は、自身の公開鍵証明書を発行したCA1(13)、CA2(14)を信頼するものとする。

【0031】

次に、図1のPKIシステムを構成する各装置について説明する。

【0032】

図2を用いて、EE装置を説明する。

【0033】

EE装置は、処理部30aと記憶部30bと、NET17を介して他装置と通信を行うための通信部36と、ユーザが作成した電子文書や他のEEから受け取った電子文書の入出力や利用者からの指示の受付を行う入出力部37と、を有する。

【0034】

処理部30aは、電子文書に対する署名を生成する署名生成部34と、署名の検証を行う署名検証部35と、EE装置の各部を統括的に制御する制御部38と、を有する。

【0035】

記憶部30bは、利用者が作成した電子文書を保持する電子文書保持部31と、秘密鍵(署名鍵)と、これと対になる公開鍵の公開鍵証明書と、当該EE装置を運用するEEが信頼するCAの自己署名証明書を保持する鍵保持部32と、他のEEから受け取った署名付きの電子文書と公開鍵証明書を保持する検証対象保持部33と、を有する。

【0036】

このような構成において、制御部38は、入出力部37を介して利用者から、電子文書保持部31に保持してある電子文書を他のEEに送信すべき旨の指示を受け付けると、当該電子文書を電子文書保持部31から読み出し、これを署名生成部34に渡す。署名生成部34は、鍵保持部32に保持されている秘密鍵を用いて渡された当該電子文書に対する署名を生成する。

【0037】

制御部38は、電子文書保持部31から読み出した電子文書に署名生成部34

で生成された署名を付して、署名付き電子文書を作成する。

【0038】

作成した署名付き電子文書と鍵保持部32に保持されている公開鍵証明書とを、通信部36を介して、利用者から指示された送信先のEEへ送信する。

【0039】

制御部38は、通信部36を介して、他のEE装置から署名付き電子文書と公開鍵証明書を受け取ると、これらを関連づけて検証対象保持部33に保持せると共に、これらの検証要求を署名検証部35に通知する。

【0040】

これを受け、署名検証部35は、検証対象保持部33に保持されている署名付き電子文書の署名を、対応する公開鍵証明書を用いて検証する。

【0041】

それから、署名検証部35は、鍵保持部32に保持されている信頼するCAであるCA1(13)の自己署名証明書から当該公開鍵証明書までのパスに含まれる証明書を、通信部36を介して各CAから取得して、パスを構築し、そのパスを検証する。そして、これらの検証により正当性が確認できた場合にのみ、署名付き電子文書を正当な物として扱い、必要に応じて入出力部37から出力する。

【0042】

次に、図3を用いてRA装置を説明する。

【0043】

RA装置は、処理部40aと記憶部40bと、NET17を介して他装置と通信を行うための通信部44と、公開鍵証明書等の入出力やRA装置操作者からの指示の受付を行う入出力部45と、を有する。

【0044】

処理部40aは、IA装置への公開鍵証明書の発行依頼や失効依頼を行うための電子文書を作成する依頼文書作成部43と、RA装置の各部を統括的に制御する制御部46と、を有する。

【0045】

記憶部40bは、RAに登録されたEEの情報を保持する登録者リスト保持部

41と、RAの秘密鍵とこれに対応する公開鍵証明書とを保持する鍵保持部42と、を有する。

【0046】

制御部46は、入出力部45を介してRA装置の操作者から、EE1の公開鍵証明書の発行要求依頼文書を、IA(12)へ送信すべき旨の指示を受け付けると、RA装置の操作者から入力された登録情報を登録者リスト保持部41へ保持させると共に、その旨を依頼文書作成部43に通知する。これを受け、依頼文書作成部43は、EE1装置(15)による署名生成に用いる秘密鍵と、それに対する検証に用いる公開鍵とを作成し、登録情報とEE1の公開鍵に対する署名を、鍵保持部42に保持されているRA(11)の秘密鍵を用いて署名を生成し、当該署名と、EE1の公開鍵と登録情報とを記述した公開鍵証明書発行依頼文書を作成する。

【0047】

そして、作成した公開鍵証明書発行依頼文書を、通信部44を介して、IA装置(12)へ送信する。

【0048】

また、制御部46は、通信部44を介してIA装置(12)から、公開鍵証明書発行要求に対して発行された証明書を受け付けると、入出力部45あるいは通信部44を介してEE1(15)に送信するか、あるいは郵送できるように入出力部45から出力する。

【0049】

また、制御部46は、入出力部45を介してRA装置操作者から、EE1(15)の公開鍵証明書の失効要求依頼文書を、IA(12)へ送信すべき旨の指示を受け付けると、その旨を依頼文書作成部43に伝える。これを受け、依頼文書作成部43は、失効依頼文書を作成し、通信部44を介してIA装置(12)へ送信する。

【0050】

また、制御部46は、通信部44を介してIA装置(12)から、公開鍵証明書の失効依頼に対する応答である確認の文書を受け付けると、登録者リスト保持

部41に保持されている登録者リストから、失効した証明書に対する登録者情報を削除する。

【0051】

次に、図4を用いてIA装置を説明する。

【0052】

図示するように、IA装置は、処理部50aと記憶部50bと、NET17を通して他装置と通信を行うための通信部55と、公開鍵証明書等の入出力やIA装置の操作者から指示を受け付ける入出力部56と、を有する。

【0053】

処理部50aは、公開鍵証明書を発行する発行部53と、発行部53が発行した公開鍵証明書の管理を行う管理部54と、IA装置の各部を統括的に制御する制御部57と、を有する。

【0054】

記憶部50bは、発行部53が発行した公開鍵証明書を保持する公開鍵証明書データベース51と、失効証明書リスト保持部52と、を有する。

【0055】

このような構成において、制御部57は、通信部55を介してRA装置(11)から公開鍵証明書の発行依頼を受け付けると、その旨を発行部53に伝える。これを受け、発行部53は、これに対する公開鍵証明書を作成する。この際、RA(11)の名称や、RA(11)の署名や、必要に応じて他の項目を記述し、自IA(12)の秘密鍵で公開鍵証明書に署名をする。そして、作成した公開鍵証明書を通信部55を介して、RA装置(11)へ送信する。また、この公開鍵証明書を公開鍵証明書データベース51に登録する。

【0056】

また、制御部57は、通信部55を介して、RA装置(11)から公開鍵証明書の失効依頼を受け付けると、その旨を管理部54に伝える。これを受け、管理部54は、失効対象の公開鍵証明書を公開鍵証明書データベース51から削除する。そして、管理部54は、失効依頼により、公開鍵証明書データベース51から削除した公開鍵証明書に関する情報が記述された失効証明書リスト(一般に

、CRL (Certification Revocation List) 、ARL (Authority Revocation List) と呼ばれている) を、定期的に作成し、これを失効証明書リスト保持部52に保持させる。なお、管理部54は、作成した失効リストに、次回の失効証明書リストの作成予定日時を記述するものとする。

#### 【0057】

また、管理部54は、公開鍵証明書データベース51に格納されている各公開鍵証明書の有効期限を調査し、有効期限を過ぎている公開鍵証明書を公開鍵証明書データベース51から削除する処理も行う。

#### 【0058】

図2～図4に示すEE装置、RA装置とIA装置の各々は、例えば、図5に示すような、CPU61と、メモリ62と、ハードディスク等の外部記憶装置63と、CD-ROM等の可搬性を有する記憶媒体69から情報を読み取れる読み取り装置64と、NET17を介して他装置と通信を行うための通新装置65と、キーボードやマウス等の入力装置66と、モニタやプリンタ等の出力装置67と、これらの各装置間のデータ送受を行うインターフェース68とを備えた、一般的な電子計算機上に構築できる。

#### 【0059】

そして、CPU61がメモリ62上にロードされた所定のプログラムを実行することにより、各処理部を実現できる。すなわち、通信部36、44、55は、CPU61が通信装置66を利用することにより、入出力部37、45、56は、CPU61が入力装置66や出力装置67や読み取り装置64を利用することにより、そして、記憶部30b、40b、50bは、CPU61がメモリ62や外部記憶装置63を利用することにより実現される。また、処理部30a、40a、50aは、CPU61のプロセスとして実現される。

#### 【0060】

上記所定のプログラムは、読み取り装置64を介して記憶媒体69から読み出され、あるいは、通信装置66を介してネットワークに接続された他の装置からダウンロードされて、外部記憶装置63に導入されるものであってもよい。

#### 【0061】

次に、上記構成のEE1(15)、RA(11)およびIA(12)が、図1に示すようなCA1(13)とEE1(15)の関係にある場合を例にとり、EE1(15)、RA(11)およびIA(12)の動作について説明する。

#### 【0062】

本実施形態のEE1(15)、RA(11)およびIA(12)の動作は、公開鍵証明書の発行動作と、失効動作とに分かれる。

#### 【0063】

上記構成のEE1(15)、RA(11)およびIA(12)が行う公開鍵証明書の発行動作を説明する。

#### 【0064】

図6は、本実施形態のEE1(15)、RA(11)およびIA(12)で行われる公開鍵証明書の発行動作を説明するためのフロー図である。

#### 【0065】

EE1装置(15)の利用者は、公開鍵証明書の発行申請に必要な情報を記載した申請書を作成し(ステップS1001(S1001と表す。以下同様。))、その申請書に記載された情報が確かなものである事を示す証明書等とともに、郵送や対面等によってRA装置(11)の操作者へ渡す(S1002)。

#### 【0066】

RA装置(11)の操作者は、公開鍵証明書発行の申請書および証明書等を受け付け(S1003)、その申請書の内容が、確かにEE1(15)の利用者に対する情報であり、公開鍵証明書を発行できる者である事を目視や対面等によって確認する(S1004)。

#### 【0067】

次に、RA装置(11)の操作者は、申請書に記載されたEE装置1(15)の利用者の登録情報を、入出力部45を介して入力し、そして当該EE1(15)に対する公開鍵証明書発行依頼をIA装置(12)へ送信すべき旨の指示を行う。依頼文書作成部43は公開鍵証明書発行依頼文書を作成する(S1005)

#### 【0068】

依頼文書作成部43の具体的な動作は、すでに説明したとおりである。図7に示すように、作成した公開鍵証明書発行依頼文書90は、登録情報91と、EE1装置(15)が電子文書の署名に使用する秘密鍵に対応する公開鍵92と、RAの名前と署名と署名対象情報が記載されたRA(11)が保証する情報93と、これらの情報(91、92、93)に対するRA(11)の署名94から構成される。

## 【0069】

依頼文書作成部43は、作成した公開鍵証明書発行依頼文書を、通信部44とNET17を介してIA装置(12)へ送信する(S1006)。

## 【0070】

IA(12)は、公開鍵証明書発行依頼文書90を、RA(11)が発行したことを見知る技術で認証し、受け付ける。(S1007)。

## 【0071】

発行部53は、公開鍵証明書発行依頼に応答して、図8に示す公開鍵証明書100を作成する(S1008)。

## 【0072】

公開鍵証明書に記載する情報には、公開鍵の発行者名であるIA(12)の名称105や、IA(12)に割り当てられた証明書のシリアル番号104などIAが設定すべき情報と、発行部53が公開鍵証明書依頼文書90に含まれる情報から抽出した、公開鍵証明書の主体者であるEE1名106や、公開鍵92や、RA(11)が保証する情報93などがある。

## 【0073】

図8に示すように、公開鍵証明書100は、基本領域101と、拡張領域102と、IA署名103と、からなり、基本領域101には、シリアル番号104と、IA名105と、EE名106と、EE1(15)の公開鍵92などが記載され、RAが保証する情報93などの、拡張領域が記載される。

## 【0074】

次に、発行部53は、基本領域101と拡張領域102の情報に対して、IAの秘密鍵で署名103を生成し、公開鍵証明書100を作成する。

## 【0075】

IA装置(12)は、作成された公開鍵証明書100を、公開鍵証明書データベース51に登録し、NET17を介してRA装置(11)に送信する(S1009)。

## 【0076】

RA装置(11)は、NET17を介して公開鍵証明書100を受け付けたら(S1010)、通信部36または入出力部37を介して、通信または郵送による安全な方法により、EE1(15)に公開鍵証明書100とそれに対する秘密鍵を渡す(S1011)。

## 【0077】

EE1装置(15)は、RA装置(11)から公開鍵証明書100と、それに対する秘密鍵を受け付け(S1012)、鍵保持部32へ保持する。

## 【0078】

次に、公開鍵証明書発行依頼文書90や、公開鍵証明書100の拡張領域102に記載される、RAが保証する情報93を、説明する。

## 【0079】

まず、図9を参照し、署名対象識別子を用いて、RAが保証する情報93を示す方法を説明する。

## 【0080】

図示するように、署名対象識別子を用いる場合、RAが保証する情報93は、RA名111と、RAが保証する情報を示す署名対象識別子112と、RAの秘密鍵で生成したRA署名113と、から構成される。

## 【0081】

署名対象識別子112を具体的に説明する。署名対象識別子は、RAがS1004で確認および審査した情報のうち、公開鍵証明書に記載される情報を示すものである。RAが保証する情報は、例えば、EE名(SubjectName)や、公開鍵(PublicKey)や、EEの属性情報などがあり、対象情報の選び方がいろいろ考えられる。そのため、対象情報の一つ以上の組み合わせを指定する識別子を一つ以上あらかじめ、システムで定めてRA、EE、IAがアクセス可能な状態で登

録しておく。RAは、この識別子が示す情報に対して署名を生成する（RAの署名113）。

#### 【0082】

上記実施形態のように、署名対象識別子を用いてRAが保証する情報部93を記載する場合、RAがどのような情報を保証するかによって署名対象識別子を登録する。そのため、様々な組み合わせを署名対象情報に指定できることから、CAの運営者のニーズに柔軟に対応することができる。

#### 【0083】

また、次に示す、署名対象情報のハッシュ値を用いる方法も可能である。

#### 【0084】

図10に示すように、署名対象情報のハッシュ値を用いる場合、RAが保証する情報93は、登録機関名121と、登録機関が保証する情報のハッシュ値部122～123と、これらの情報に対してRA（11）の秘密鍵で生成した登録機関名124と、から構成される。

#### 【0085】

登録機関が保証する情報のハッシュ値部122～123は、RA（11）がS1004で確認および審査した情報のうち、公開鍵証明書に記載される情報のそれぞれのハッシュ値が記載される。RAが保証する情報は、例えば、EEの名称(subjectName)や、公開鍵(publicKey)や、その他のEEの属性情報がある。

#### 【0086】

RA（11）は、RA名121と、登録機関が保証する情報のハッシュ値部122～123に対して、署名を生成する（登録機関の署名124）。

#### 【0087】

署名対象情報のハッシュ値を用いて、RAが保証する情報部93を記載する場合、各署名対象情報のハッシュ値に対して、証明書に記載された情報と対応しているかを確認する必要があるものの、署名対象識別子を登録すること無しに署名による保証対象情報を示すことができる。

#### 【0088】

次に、RA（11）およびRAの公開鍵証明書発行機関における、RA（11

) の公開鍵証明書の失効動作について説明する。

【0089】

RA(11)の運営者(責任者)は、RA(11)の公開鍵証明書を失効させる場合、公開鍵証明書失効依頼文書を確実な方法(通信による署名付文書の送付や、手渡し等)でRAの公開鍵証明書発行機関へ送付する。

【0090】

RA(11)の公開鍵証明書発行機関は、公開鍵証明書失効依頼文書を、RA(11)が発行したことを周知の技術で認証し、受け付ける。

【0091】

RA(11)の公開鍵証明書発行機関は、周知の技術でRA(11)の公開鍵証明書を失効させる。すなわち、RA(11)の公開鍵証明書発行機関のデータベースからRA(11)の公開鍵証明書を削除し、証明書発行機関の署名が付与された証明書失効リストを定期的に発行する。

【0092】

このように、本実施形態による公開鍵証明書は、RAの公開鍵証明書を失効させることにより、RA毎に一括で有効でないものとできる。この方法により、全てのEEの公開鍵証明書を失効させる場合に比べて、証明書失効リストの容量が削減できる。

【0093】

次に、図1に示す構成において、EE2装置(16)がEE1装置(15)の公開鍵証明書を検証する場合の動作を説明する。

【0094】

EE2装置(16)は、EE1装置(15)から、署名付き電子文書と公開鍵証明書を受け付けると、上述の通り、その電子文書の署名検証と、公開鍵証明書の検証を行う。

【0095】

図11は、EE2装置(16)の署名検証部35が行う公開鍵証明書の検証動作を説明するためのフロー図である。

【0096】

署名検証部35は、EE2から公開鍵証明書の検証の指示を受け付けると、EE2装置(16)の信頼する認証局CA2(14)の自己署名証明書から、EE1(15)の公開鍵証明書までのパスを構築する(S3001)。

#### 【0097】

具体的には、EE2装置(16)の署名検証部35は、EE1(15)の公開鍵証明書から、当該証明書の発行機関名の情報(IA名)を得る。

#### 【0098】

そして、IA装置(12)の公開鍵証明書データベース181へアクセスし、CA2(14)からIA(12)へ発行された公開鍵証明書を得て、鍵保持部32に保持する。

#### 【0099】

CA2(14)は、EE2(16)の信頼する認証局であるため、EE1装置(15)から送付されたEE1(15)の公開鍵証明書と、IA装置(12)から入手したIA(12)の公開鍵証明書と、鍵保持部32に保持されているCA2(14)の自己署名証明書を集めることにより、認証パスが構築できたことになる。

#### 【0100】

署名検証部35は、各証明書の検証を行うことにより、S3001で構築されたパスについて、以下の通り検証を行う。(S3002)

署名検証部35は、CA2(14)の自己署名証明書に含まれるCA2(14)の公開鍵を用いて、IA(12)の公開鍵証明書に付与された署名の検証を行うと共に、これらの公開鍵証明書の内容が整合しているかを確認する。次に、IA(12)の公開鍵証明書に含まれるIA(12)の公開鍵を用いて、EE1の公開鍵証明書に付与された署名の検証を行うと共に、これらの公開鍵証明書の内容が整合しているかを確認する。

#### 【0101】

以上のように、認証パスを構成する全ての証明書に関して、署名検証と整合性を確認することにより、パスの検証を行う。

#### 【0102】

次に、署名検証部35は、検証対象の公開鍵証明書に記載されたRAを特定する情報（例えばRA名）に基づいて、RA(11)の公開鍵証明書をその発行機関のデータベースから入手し、そのRAの公開鍵証明書に含まれるRA(11)の公開鍵を用いて、EE1(15)の公開鍵証明書の拡張領域に記載されたRAの署名を検証する。(S3003)

また、RAの公開鍵証明書は、検証対象の公開鍵証明書の拡張領域に記載しておくことにより、検証者が入手する方法も可能である。

#### 【0103】

署名検証部35は、S3003で用いたRA(11)の公開鍵証明書へのパスを構築する(S3004)。

#### 【0104】

すなわち、EE2(16)の信頼するCA2(14)から、RA(11)までのパスを構築する。このRA(11)までのパスは、RA(11)の公開鍵証明書がどこから発行されているかによって異なる。

#### 【0105】

まず、図14に示すように、RA(11)の公開鍵証明書が、IA(12)から発行されている場合において、RA(11)の公開鍵証明書までのパスを構築する例について説明する。

#### 【0106】

署名検証部35は、RA(11)の公開鍵証明書から、当該証明書を発行したIAの情報を得る。

#### 【0107】

そして、その発行したIA装置(12)の公開鍵証明書データベース181にアクセスし、IA(12)がCA2(14)から発行された公開鍵証明書を得る。

#### 【0108】

CA2(14)は、EE2(16)が信頼する認証局であるため、認証パスを構成する証明書は、S3003で用いたRA(11)の公開鍵証明書と、IA装置(12)の公開鍵証明書データベース181から入手したIA(12)の公開

鍵証明書と、鍵保持部32に保持されているCA2(14)の自己署名証明書となる。

#### 【0109】

ここで、IA(12)の公開鍵証明書と、CA2(14)の自己署名証明書は、S3001で既に使用されているため、本ステップで再度利用することができるものとする。

#### 【0110】

EE2装置(16)の制御部38は、S3002と同様の方法にて、S3004において構築されたRA(11)までのパスの検証を行う(S3005)。

#### 【0111】

以上のS3002、S3003、S3005における全ての検証に成功した場合、EE1(15)の公開鍵証明書の有効性が確認できることになる。確認結果は、EE2装置(16)の入出力部37を介して、利用者に示される(S3006)。

#### 【0112】

また、上記実施形態とは異なり、図15に示すように、RA(11)の公開鍵証明書が、CA2(14)と相互認証を行っているCA3(192)から発行されていてもよい。その場合は、以下のように、RA(11)の公開鍵証明書までのパスを構築する。

#### 【0113】

署名検証部35は、S3003で用いたRA(11)の公開鍵証明書から、RA(11)の公開鍵証明書の発行機関CA3(192)の情報を入手する。そして、そのCA3(192)の公開鍵証明書データベース(193)へアクセスし、CA3(192)がCA2(14)から発行された証明書を入手する。

#### 【0114】

CA2(14)は、EE2(16)の信頼する認証局であるため、認証パスを構成する公開鍵証明書は、S3003で用いたRA(11)の公開鍵証明書と、CA3(192)の公開鍵証明書データベース193から入手したCA3(192)の公開鍵証明書と、鍵保持部32に保持されているCA2(14)の自己署

名証明書となる。

【0115】

また、RAの署名の検証方法は、RA(11)が保証する情報部93を示す方法によって異なる。

【0116】

まず、署名対象識別子を用いて、RAが保証する情報部93を示す場合において、RAの署名113を検証する方法を示す。

【0117】

図12は、署名対象識別子を用いた場合において、EE2(16)が、RAの署名113の検証を行う動作を説明するためのフロー図である。

【0118】

EE2(16)の署名検証部35は、EE1(15)の公開鍵証明書に記載される署名対象識別子112が示す項目（図9の例では登録機関名、EE名、公開鍵を示す）を、当該公開鍵証明書から集め（S4001）、そのハッシュ値を取る（S4002）。それと共に、RA(11)の公開鍵証明書に記載された公開鍵を用いて、EE1(15)の公開鍵証明書に記載されたRAの署名113を復号化する（S4003）。そして、S4002とS4003からそれぞれ出力される値を比べ、等しいかどうかを確認する（S4004）。

【0119】

この結果が等しければ、RAの署名113が有効であることを検証できたことを意味する（S4005）。逆に、等しくない場合、RAの署名113が有効でないことを意味する（S4006）。

【0120】

次に、署名対象情報のハッシュ値を用いて、RAが保証する情報部93を示す場合における、登録機関の署名124の検証方法を示す。

【0121】

図13は、署名対象情報のハッシュ値を用いた場合において、EE2(16)が、RAの署名113の検証を行う動作を説明するためのフロー図である。

【0122】

EE2(16)の署名検証部35は、RA名121と、署名対象情報のハッシュ値部122～123に対して、ハッシュ値を取る(S5001)。それと共に、RA(11)の公開鍵証明書に記載された公開鍵を用いて、EE1(15)の公開鍵証明書に記載されたRAの署名124を復号化する(S5002)。そして、S5001とS5002からそれぞれ出力される値を比べ、等しいかどうかを確認する(S5003)。これらの値が等しくない場合、RAの署名124は有効でないことになる(S5006)。等しい場合はS5004へ進む。

#### 【0123】

S5004では、登録情報のハッシュ値部122～123の各値が、公開鍵証明書の各情報と対応しているかを確認する。すなわち、公開鍵証明書のEE名106のハッシュを取った値と、EE名のハッシュ値122が同じであることを確認し、同様に公開鍵92のハッシュ値を取った値と、公開鍵のハッシュ値123が同じであることを確認する。

#### 【0124】

この結果が等しければ、RAの署名124が有効であることを検証できたことを意味する(S5005)。逆に、等しくない場合、RAの署名124は有効でないことを意味する(S5006)。

#### 【0125】

以上、本発明の実施形態について説明した。

#### 【0126】

上記の各実施形態では、EE1(15)の公開鍵証明書の拡張領域に、RA(11)の署名113(または124)を含んだRAの保証する情報部93を記載している。そして、その公開鍵証明書を受け取った他のEEは、当該公開鍵証明書のRAの署名を検証することで、そのRAが保証する情報部93が示す記載事項がRA(11)により保証されていることを確かめることができる。すなわち、公開鍵証明書に記載されたEE1(15)は、RA(11)により本人確認および審査されたことを、その公開鍵証明書を受け取ったEEが確認することができる。RAが保証する情報部93が示す記載事項以外の事項は、当該公開鍵証明書のIAの署名を検証することで、IAにより保証されていることになる。

## 【0127】

なお、本発明は、上記の実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

## 【0128】

例えば、上記の実施形態では、一箇所のRAで本人確認および審査を行う形態であるが、本発明はこれに限定されない。EE1(15)の本人確認および審査を、複数のRAで行い、公開鍵証明書の拡張領域に、各RAで確認された情報が何かを示すために、RAが保証する情報部93を、複数記載してもよい。

## 【0129】

また、上記実施形態においては、公開鍵証明書に、検証者が署名対象範囲を知ることができる情報が含まれていた。これらに対し、公開鍵証明書に記載する情報のうち、RAが保証する署名対象情報をシステム内であらかじめ決めておく方法を用いても良い。その場合、RA(11)は、あらかじめ指定された情報に対してRA(11)の署名を生成する。RAが保証する情報部93には、RAの名前と署名を記載するだけで良い。

## 【0130】

この方法における、登録機関の署名の検証方法を示す。

## 【0131】

まず、あらかじめ署名対象情報として指定されている項目を、公開鍵証明書から集め、それに対してハッシュ値をとる。そして、登録機関の署名をRAの公開鍵で復号化し、上記の値と同じであるかを調べる。この結果が等しければ、RAの署名が有効であることを確認できたことを意味する。逆に、等しくない場合、RAの署名は有効でないことを意味する。

## 【0132】

RAが、あらかじめ指定されている場合、署名対象情報のハッシュ値が公開鍵証明書のどの項目に対応しているかを確認する必要がないため、署名対象情報のハッシュ値を取る場合に比べて検証処理が軽減される。

## 【0133】

【発明の効果】

本発明によれば、公開鍵証明書に記載される情報のうち、登録機関が保証する情報の範囲および内容を、それを受け取ったEEが確認することができる。すなわち、その公開鍵証明書の内容（誰が何を保証しているか）を、EEが確認することができる。

【図面の簡単な説明】

【図1】

本発明の一実施形態が適用されたPKIシステムの構成図である。

【図2】

図1に示すEEの概略構成を示す図である。

【図3】

図1に示すRAの概略構成を示す図である。

【図4】

図1に示すIAの概略構成を示す図である。

【図5】

図2～図4に示すEE、RAおよびIAの各々のハードウェア構成例を示す図である。

【図6】

図1に示すEE1、RAおよびIAで行われる公開鍵証明書の発行動作を示すためのフロー図である。

【図7】

図6のステップS1005で作成される公開鍵証明書発行依頼文書の概略構成を示す図である。

【図8】

図6のステップS1009で作成される公開鍵証明書の概略構成を示す図である。

【図9】

図8に示す情報93を署名対象識別子を用いて示す場合の概略構成を示す図である。

【図10】

図8に示す情報93を登録情報のハッシュ値を用いて示す場合の概略構成を示す図である。

【図11】

図1に示すEE2が、EE1の公開鍵証明書を検証する動作を示すためのフロー図である。

【図12】

署名対象識別子を用いてRAが保証する情報93を示した場合において、RAの署名113の検証動作を示すためのフロー図である。

【図13】

登録情報のハッシュ値を用いてRAが保証する情報93を示した場合において、RAの署名124の検証動作を示すためのフロー図である。

【図14】

RAの証明書がIAから発行されている場合の概略構成を示した図である。

【図15】

RAの証明書が、他の認証局であるCA3から発行されている場合の概略構成を示した図である。

【符号の説明】

11…RA、12, 205…IA、13…CA1、14…CA2、15…EE1、16…EE2、17…NET、30a, 40a, 50a…処理部、  
30b, 40b, 50b…記憶部、31…電子文書保持部、32, 42…鍵保持部、33…検証対象保持部、34…署名生成部、35…署名検証部、36, 44, 55…通信部、37, 45, 56…入出力部、38, 46, 57…制御部、41…登録者リスト保持部、43…依頼文書作成部、51…公開鍵証明書データベース、52…失効証明書リスト保持部、53…発行部、54…管理部、61…CPU、62…メモリ、63…外部記憶装置、64…読み取り装置、65…通信装置、66…入力装置、67…出力装置、68…インターフェース、69…記憶媒体

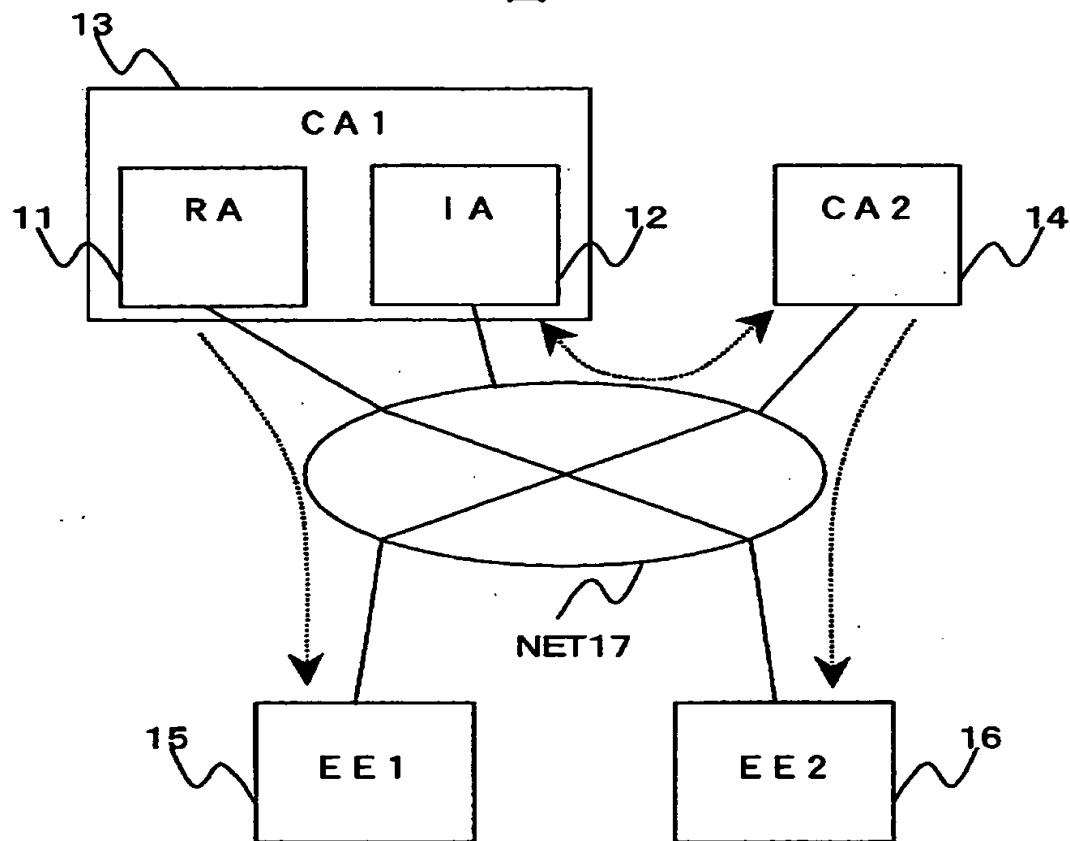
91…登録情報、92…公開鍵、93…RAが保証する情報、94…RAの署名、101…基本領域、102…拡張領域、103…IAの署名、104…

…シリアル番号、105…IA名、106…EE名、111、121…RA名、112…署名対象識別子、113、124…RAの署名、122…EE名のハッシュ値、123…公開鍵のハッシュ値、181、193…証明書データベース、192…CA3、201、211…RA1、202、212…RA2、203、217…アウトソーシング先機関、204…IAの秘密鍵、213…IA1、214…IA2、215…IA1の秘密鍵、216…IA2の秘密鍵。

【書類名】 図面

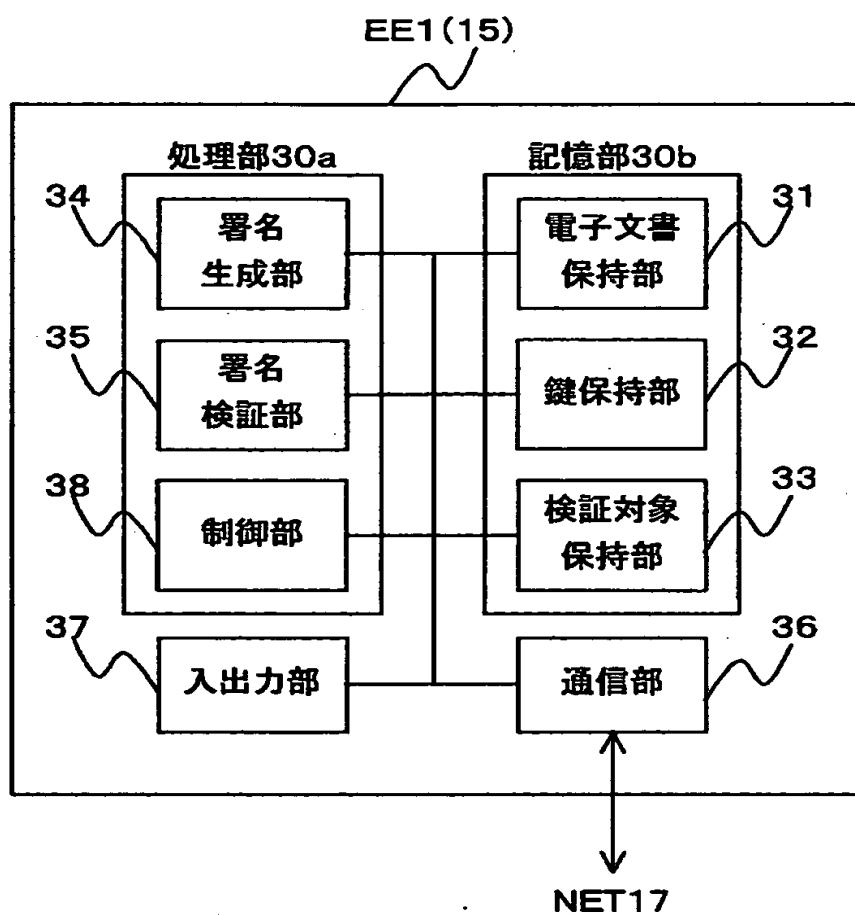
【図1】

図1



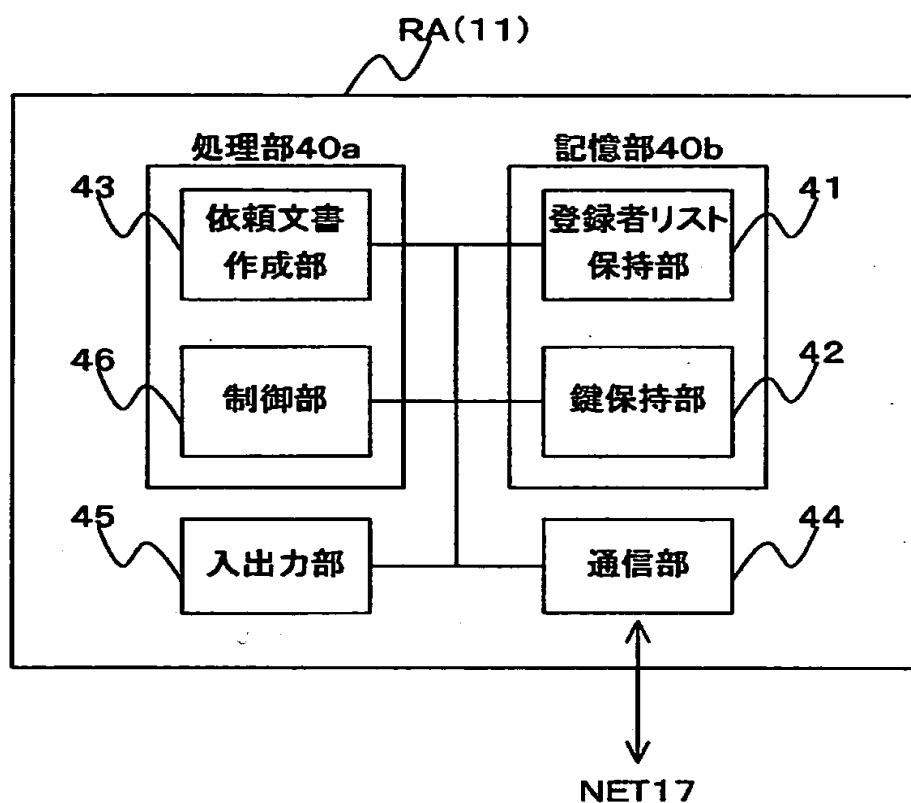
【図2】

図2



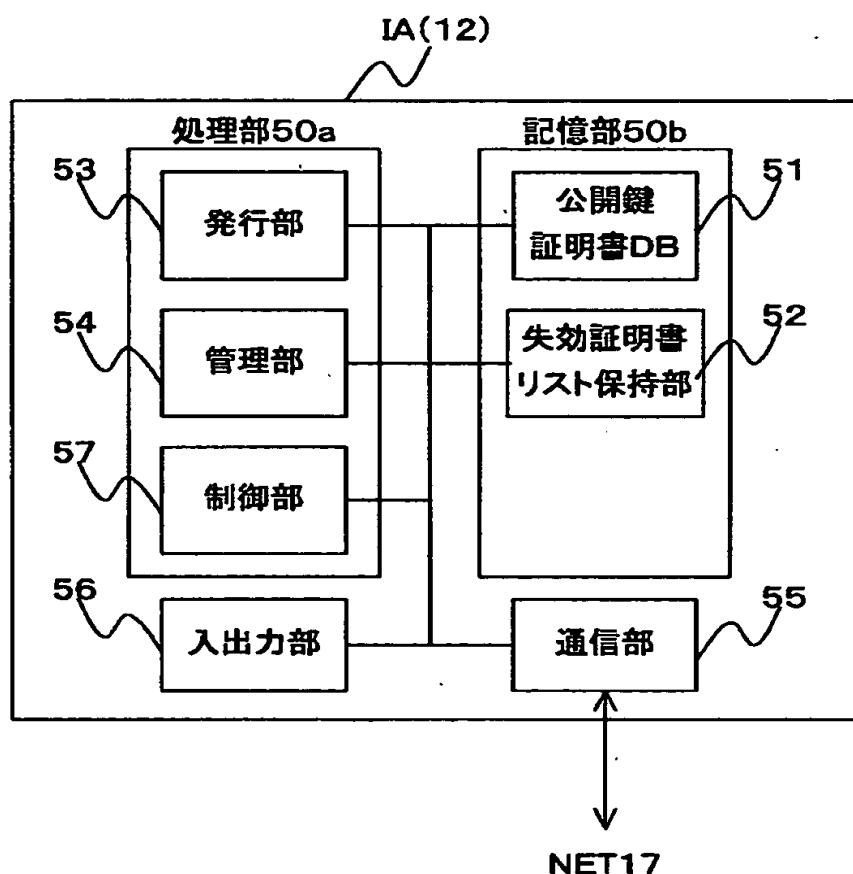
【図3】

図3



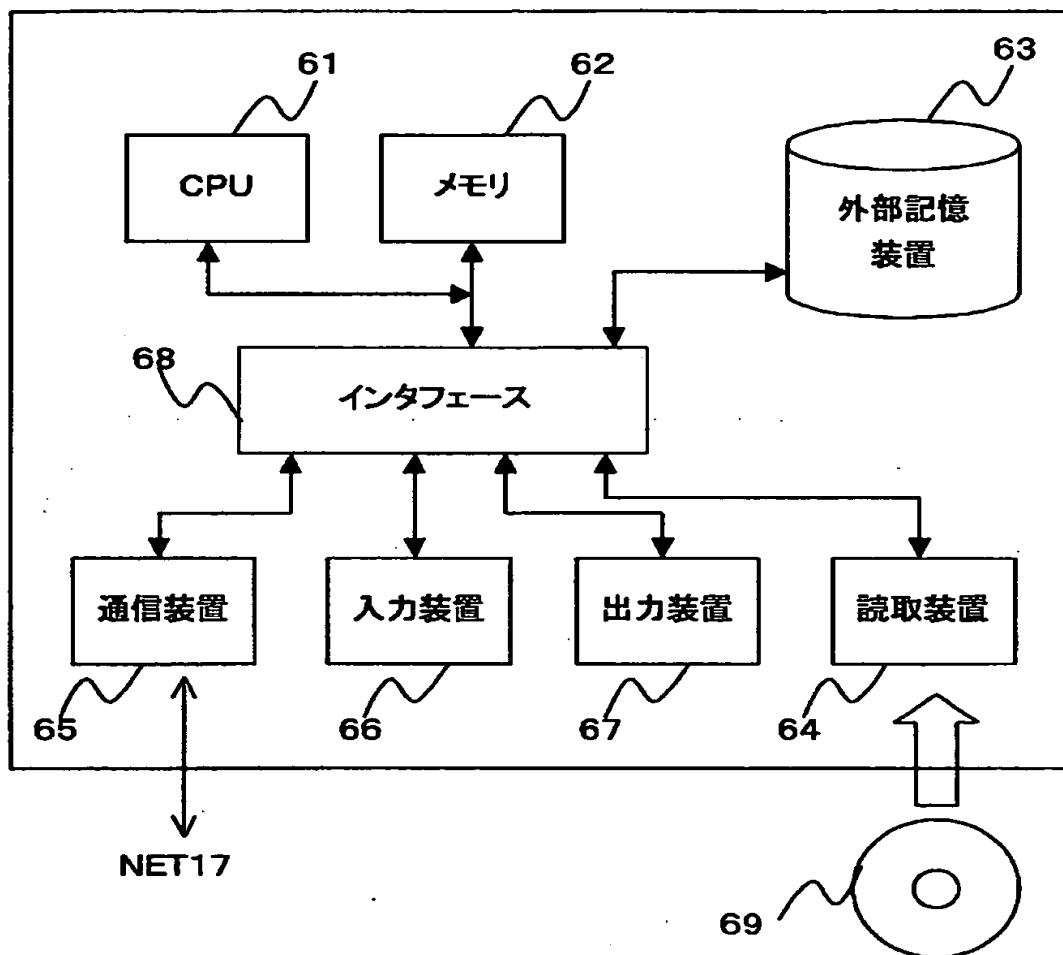
【図4】

図4



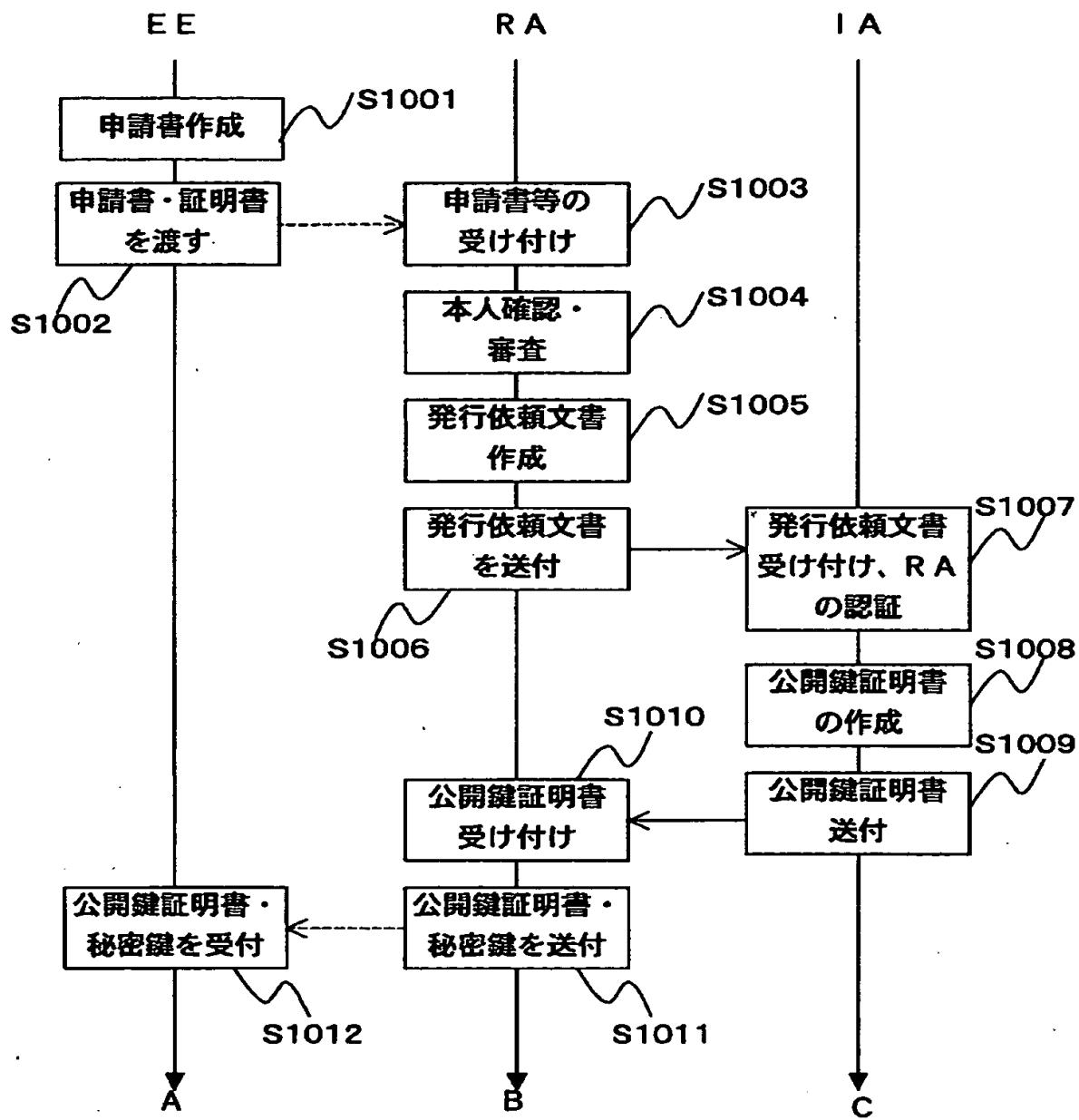
【図5】

図5



【図6】

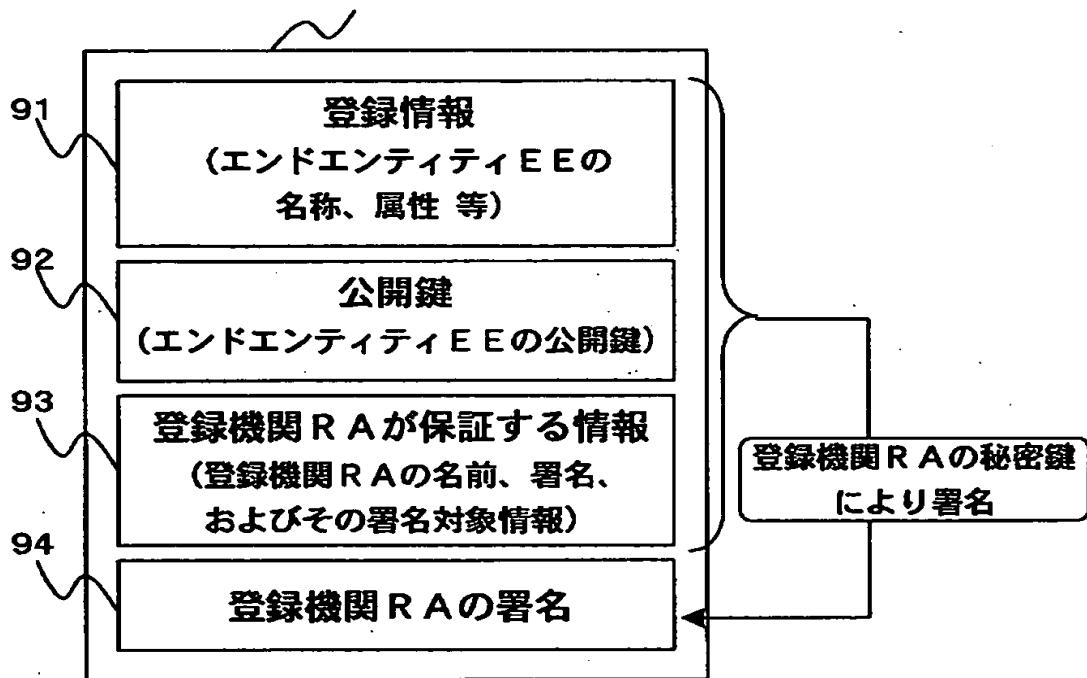
図6  
公開鍵証明書の発行動作



【図7】

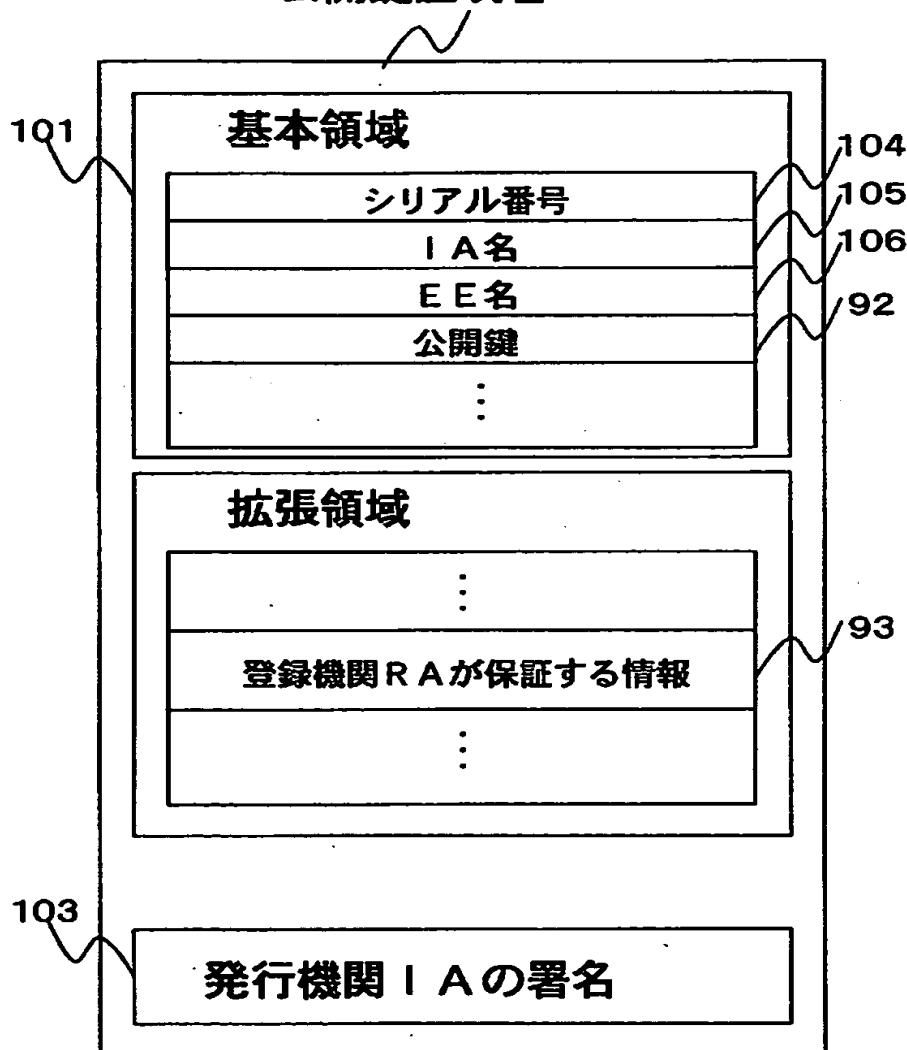
図7

## 公開鍵証明書発行依頼文書 90



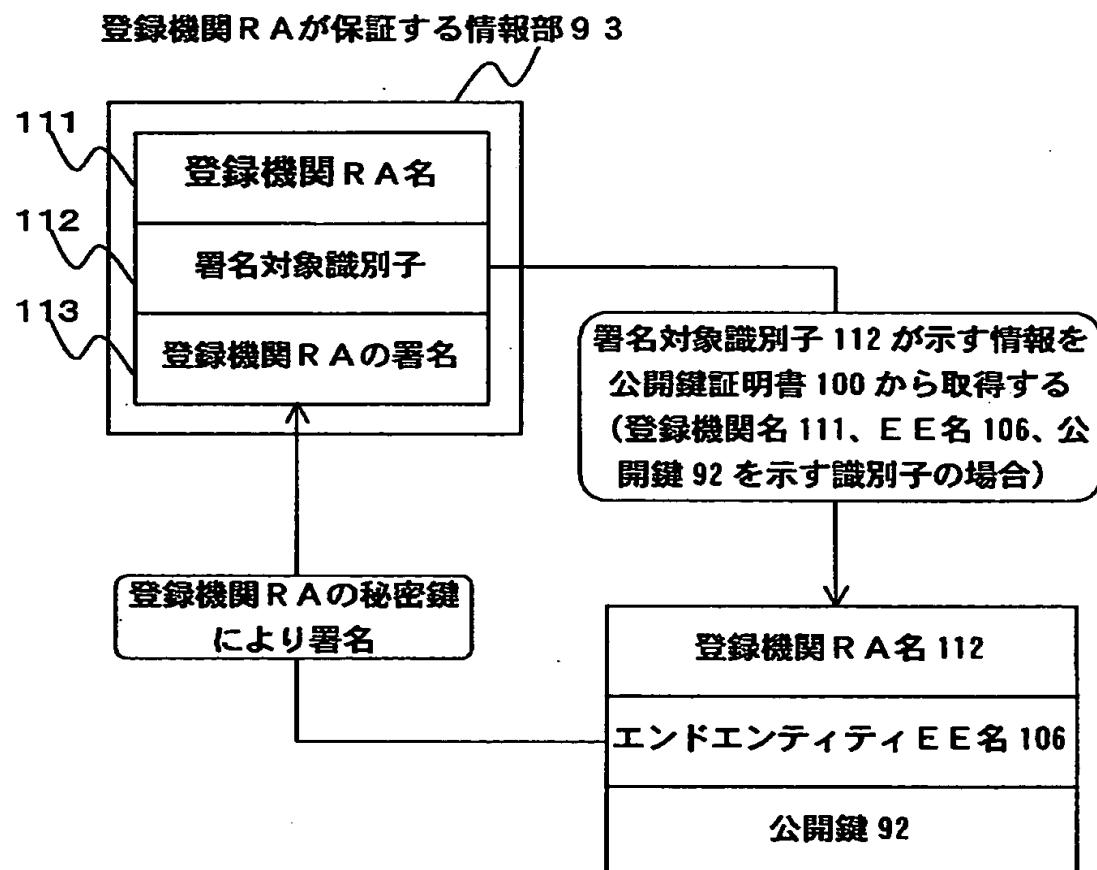
【図8】

図8  
公開鍵証明書100



【図9】

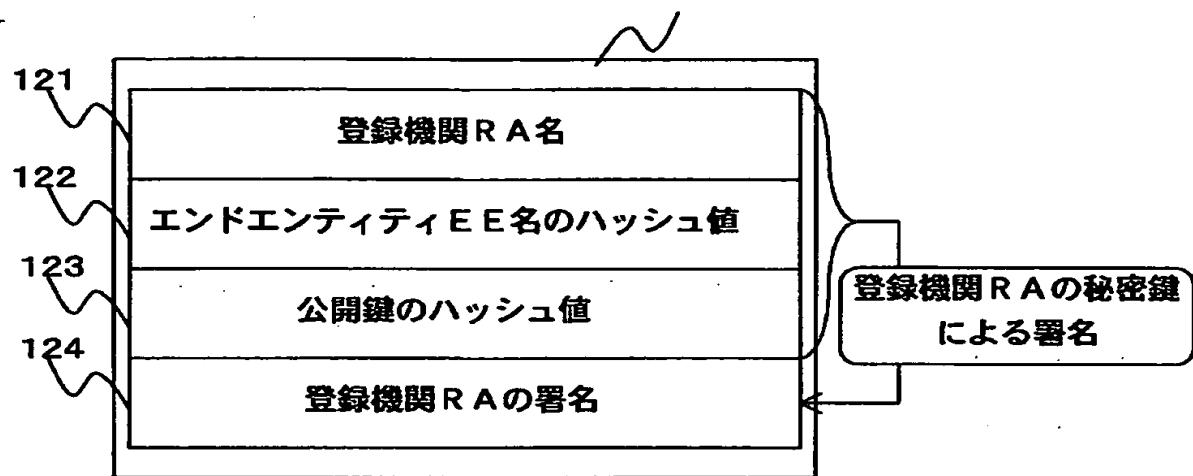
図9



【図10】

図10

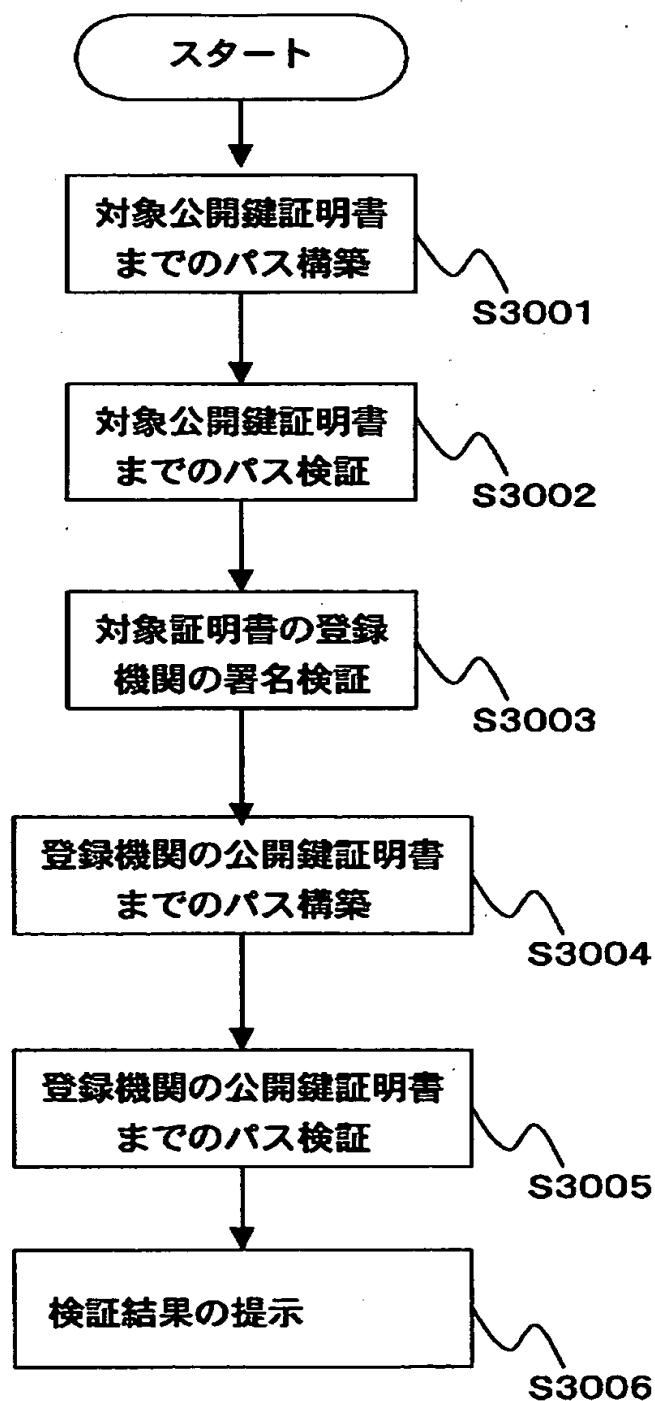
登録機関RAが保証する情報部93



【図11】

図11

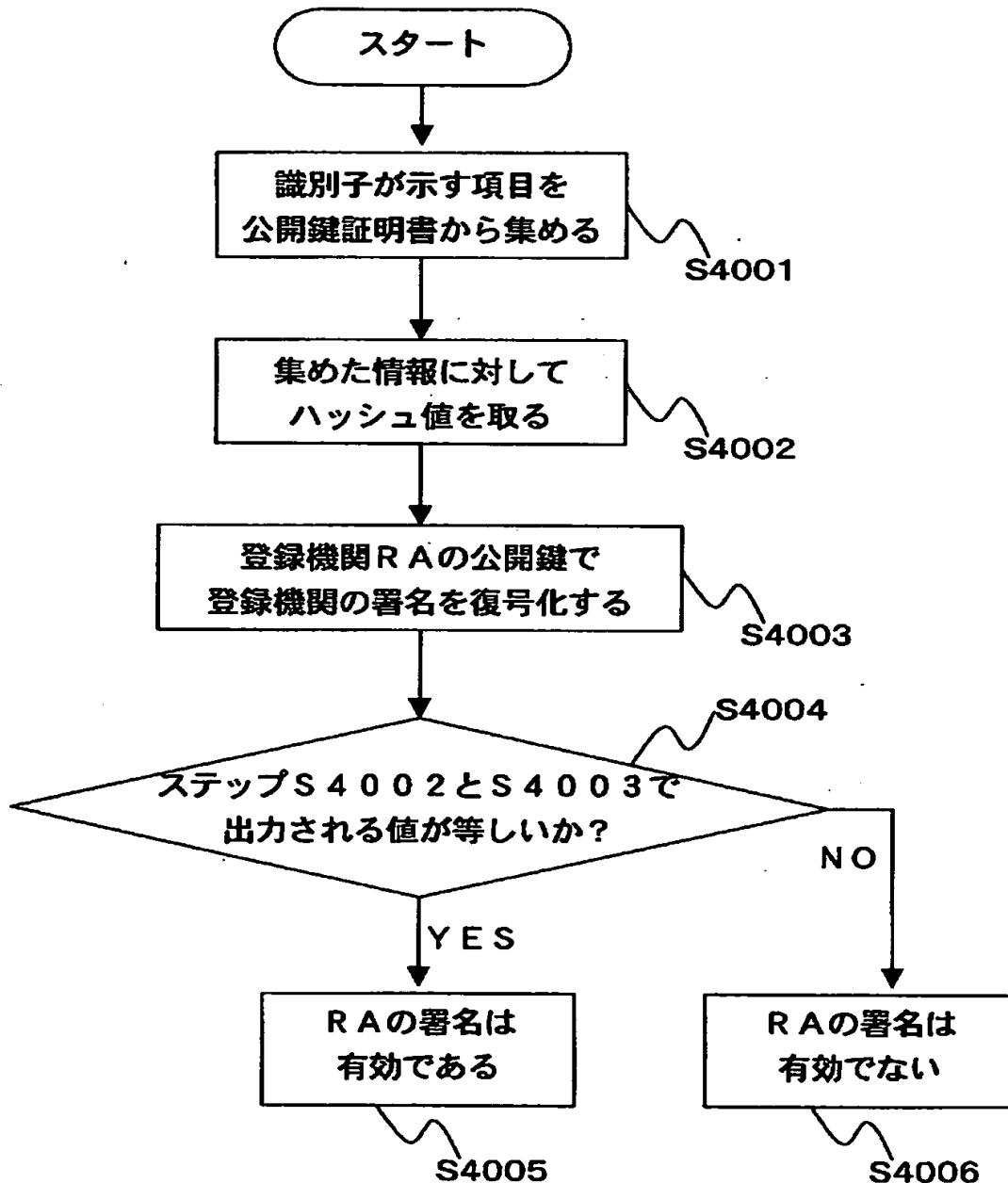
## 公開鍵証明書の検証動作



【図12】

図12

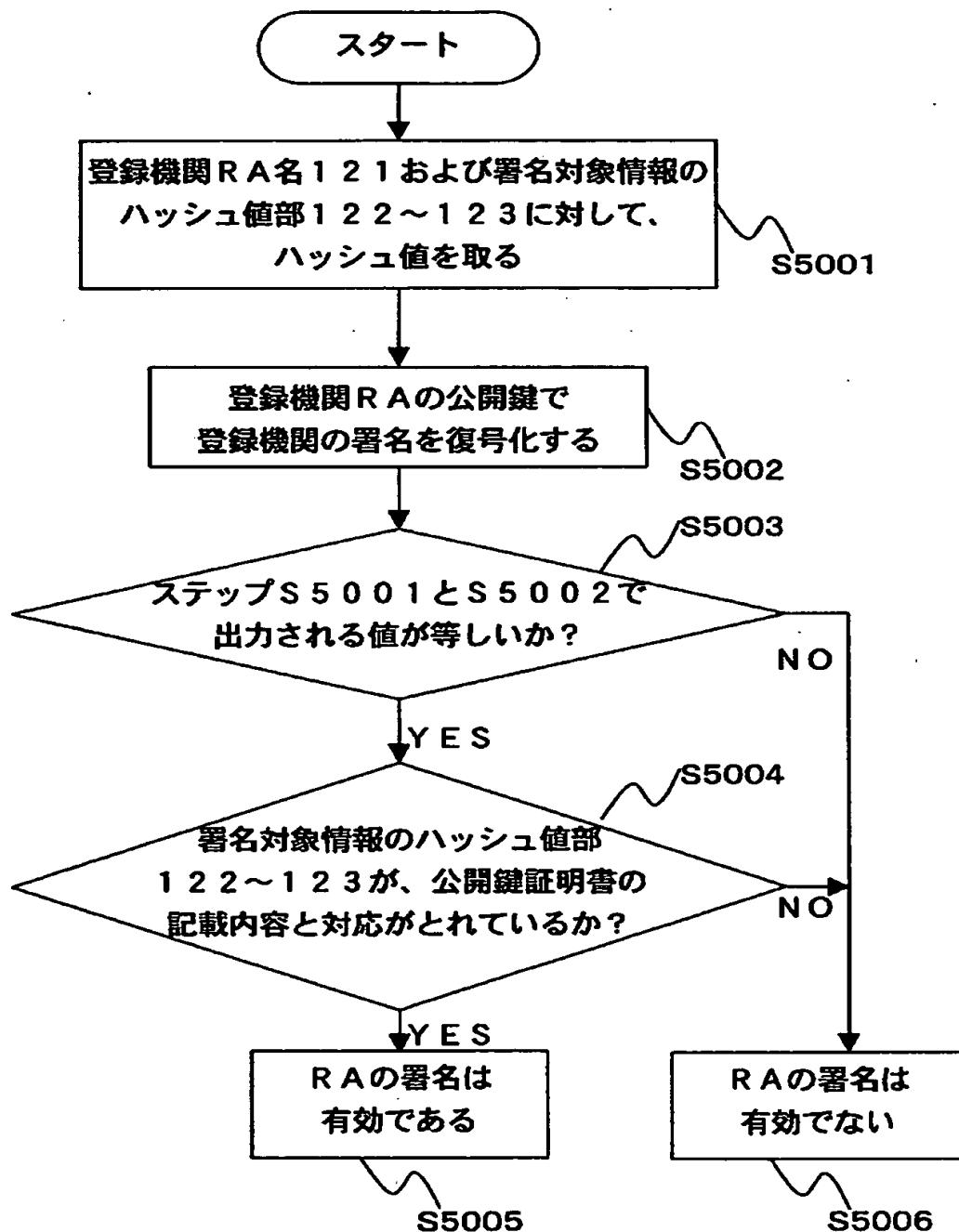
登録機関RAの署名の検証動作  
(識別子を用いた場合)



【図13】

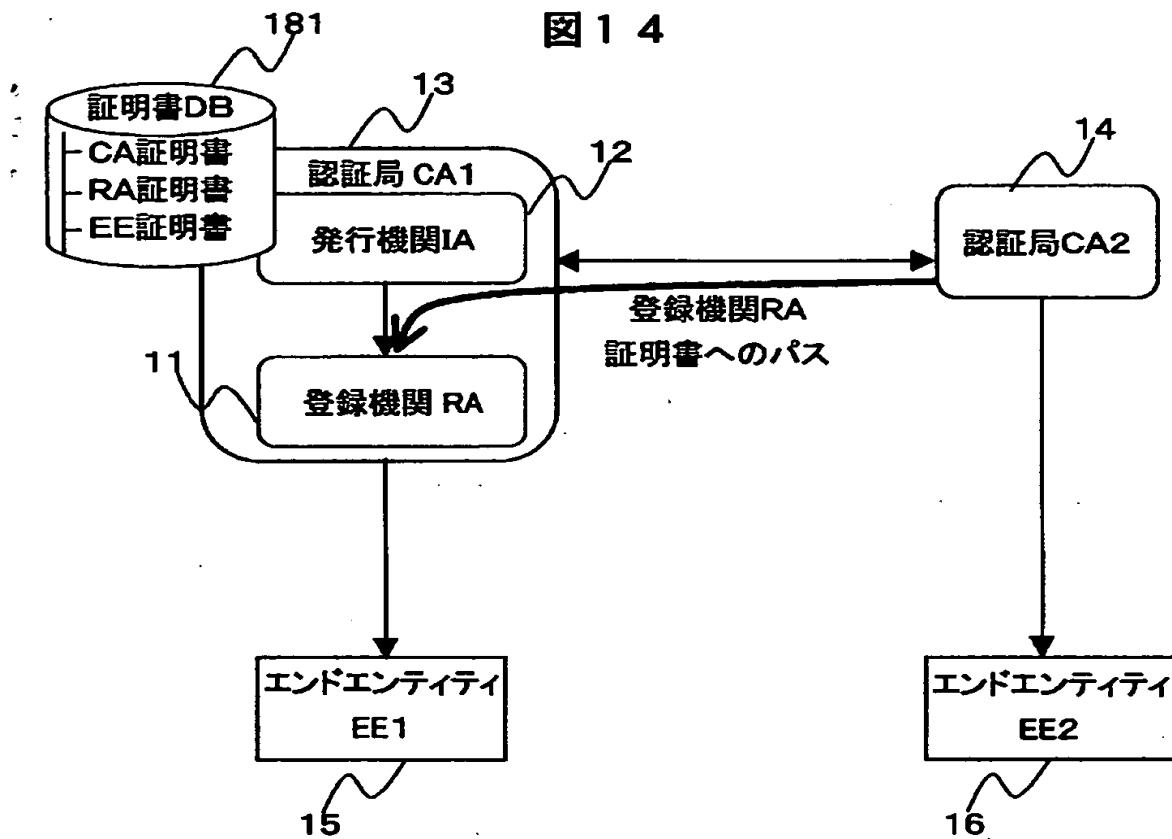
図13

登録機関RAの署名の検証動作  
(署名対象情報のハッシュ値を用いた場合)



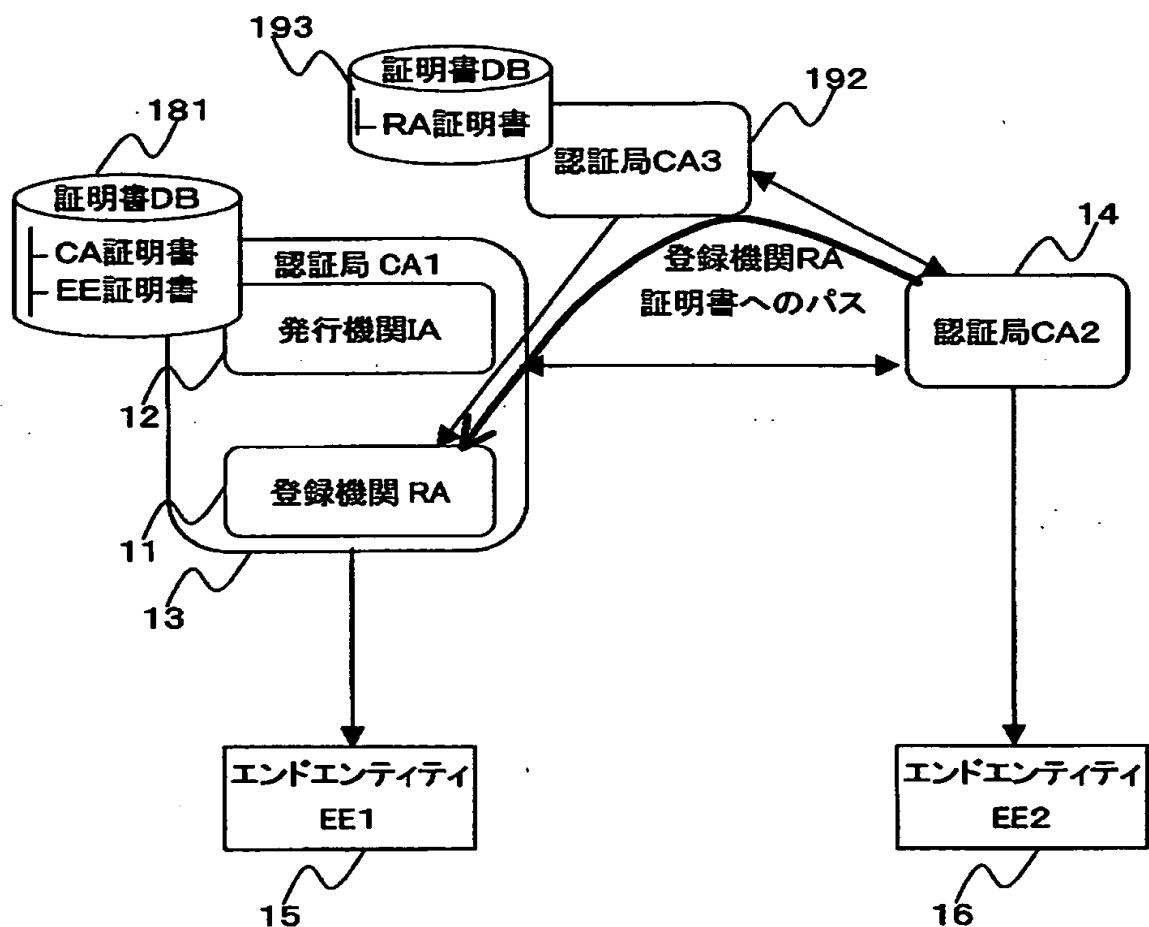
【図14】

図14



【図15】

図15



【書類名】 要約書

【要約】

【課題】

IAとRAの運営主体が異なる場合において、公開鍵証明書の証明する内容や、IAとRAの責任範囲がEEに明確に示される公開鍵証明書を発行するとともに、その公開鍵証明書の有効性確認を可能にする。

【解決手段】

RAは、EEの登録において本人確認および審査を行い、それらの情報に対して、RAの署名を生成する。IAでは、RAからの依頼により、RAの署名を含んだ公開鍵証明書を作成し、その公開鍵証明書全体に対してIAの署名を付与する。このようにして発行された公開鍵証明書を受け取ったは、RAの署名と、IAの署名を検証することにより、RAにより確認された情報が確かにRAによって保証（署名）されていることを確認するとともに、当該証明書の有効性を確認する。

【選択図】 図8

認定・付加情報

特許出願の番号	特願2001-356851
受付番号	50101716677
書類名	特許願
担当官	第八担当上席 0097
作成日	平成13年11月26日

<認定情報・付加情報>

【提出日】 平成13年11月22日

次頁無

出願人履歴情報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地

氏 名 株式会社日立製作所